IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: **8293**
Pinder *et al.*	Group Art Unit: **2432**
Serial No.: **10/015,351**	Examiner: **Nobahar, Abdulhakim**
Filed: **December 11, 2001**	Docket No.: **A-7274**

For: **ENCRYPTING RECEIVED CONTENT**

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. § 41.37 is submitted in support of the Notice of Appeal filed November 5, 2008, responding to the final Office Action mailed July 8, 2008 and the Advisory Action mailed October 28, 2008.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor are hereby authorized to be charged to Deposit Account No. 19-0761.

I. Real Party in Interest

The real party in interest of the instant application is Scientific-Atlanta, Inc., having its principal place of business at 5030 Sugarloaf Parkway, Lawrenceville, GA 30044. Scientific-Atlanta, Inc., the assignee of record, is wholly owned by Cisco Systems, Inc.

II. Related Appeals and Interferences

There are no related appeals or interferences.

III. Status of Claims

Claims 55-76, 83-91, and 105-124 stand finally rejected. No claims have been allowed. Claims 1-54, 77-82, and 92-104 have been canceled. The rejections of claims 55-76, 83-91, and 105-124 are appealed.

IV. Status of Amendments

Claims 1-54, 77-82, and 92-104 have been cancelled subsequent to the final Office Action mailed on July 8, 2008. The Advisory Action mailed on October 28, 2008 entered the amendments for the purposes of appeal. No other amendments have been made subsequent to the final Office Action mailed on July 8, 2008. The claims in the attached Claims Appendix (see below) reflect the present state of Appellants' claims.

V. Summary of Claimed Subject Matter

The claimed inventions are summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter described in the following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Embodiments according to independent claim 55 describe a method for securely storing encrypted programming received at a receiver in a subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets. The method comprises receiving a first ciphertext packet having multiple layers of encryption thereon at the receiver. *See e.g.* Appellants' specification, page 32, lines 3-9 and page 41, lines 4-5. The method further comprises applying a cryptographic algorithm to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet. *See e.g.* Appellants' specification, page 32, lines 22-26 and page 41, lines 5-12.

Embodiments according to independent claim 69 describe a method for providing a subscriber of a subscriber network with a program, the subscriber network including a headend with a plurality of receivers coupled thereto. At the headend, the method comprises receiving a first ciphertext packet. *See e.g.* Appellants' specification, page 39, line 27-28. At the headend, the method further comprises applying a cryptographic algorithm with a key to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received at the headend to a cleartext packet. *See e.g.* Appellants' specification, page 40, lines 3-7. At the headend, the method further comprises transmitting the second ciphertext packet. *See e.g.* Appellants' specification, page 37, lines 15-16. At the receiver, the method comprises receiving the second ciphertext packet having multiple layers of encryption thereon. *See e.g.* Appellants' specification, page 41, lines 4-5. At the receiver, the method further comprisesapplying a second cryptographic algorithm to the second ciphertext

packet to convert the second ciphertext packet to a third ciphertext packet without first converting the second ciphertext packet to a cleartext packet. *See e.g.* Appellants' specification, page 41, lines 4-12.

Embodiments according to independent claim 83 describe a receiver in a subscriber network that receives encrypted programming from a headend of the subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets. The receiver comprises a port adapted to receive a first ciphertext packet of the encrypted programming, the first ciphertext packet corresponding to a cleartext packet having multiple layers of encryption thereon. *See e.g.* Appellants' specification, page 23, lines 25-29, page 32, lines 3-9, and page 41, lines 4-5. The receiver further comprises a key generator adapted to generate an encryption key. *See e.g.* Appellants' specification, page 30, lines 29-34 and FIG. 7, item 708. The receiver further comprises a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to apply a cryptographic algorithm using the encryption key to the first ciphertext packet to convert the ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet. *See e.g.* Appellants' specification, page 32, lines 22-26, page 41, lines 5-12, and FIG. 7, item 610.

Embodiments according to independent claim 105 describe a method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets. The method comprises receiving from a headend of the subscriber network a first ciphertext packet at the receiver and a first key, a second key and a third key, wherein the first ciphertext packet has three layers of encryption thereon that were applied by a first cryptographic algorithm using the first key, the second key and the third key. *See e.g.* Appellants' specification, page 37, lines 15-30. The method further comprises generating a fourth key. *See e.g.* Appellants' specification, page 38, lines 17-18. The method further comprises applying to the first ciphertext packet a

second cryptographic algorithm with the first key to convert the first ciphertext packet to a second ciphertext packet having two layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet. *See e.g.* Appellants' specification, page 37, line 29 – page 38, line 2. The method further comprises applying to the second ciphertext packet a third cryptographic algorithm with the fourth key to convert the second ciphertext packet to a third ciphertext packet having a third layer of encryption thereon without first converting the second ciphertext packet to a cleartext packet. *See e.g.* Appellants' specification, page 38, lines 3-9.

Embodiments according to independent claim 110 describe a receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets. The receiver comprises an input port adapted to receive a first key, a second key, a third key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has three layers of encryption thereon that were applied by a first cryptographic algorithm using the first key, a second key and a third key. *See e.g.* Appellants' specification, page 23, lines 25-29 and page 37, lines 15-30. The receiver further comprises a key generator adapted to generate a fourth key. *See e.g.* Appellants' specification, page 38, lines 17-18 and FIG. 7, item 708. The receiver further comprises a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a second cryptographic algorithm and the first key without first converting the first ciphertext packet received from the headend to a cleartext packet and thereafter to convert the second ciphertext packet to a third ciphertext packet using a third cryptographic algorithm and the fourth key without first converting the second ciphertext packet to a cleartext packet. *See e.g.* Appellants' specification, page 38, lines 3-9 and FIGS. 6-7, item 610. The receiver further comprises a storage device in communication with the cryptographic device adapted to store the third ciphertext packet and

the second, third and fourth keys. *See e.g.* Appellants' specification, page 26, line 31 – page 27, line 11 and FIG. 6, item 614.

Embodiments according to independent claim 115 describe a method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets. The method comprises receiving from a headend of the subscriber network a first ciphertext packet at the receiver and a first key and a second key, wherein the first ciphertext packet has two layers of encryption thereon that were applied by a first cryptographic algorithm using the first key and a second cryptographic algorithm using the second key. *See e.g.* Appellants' specification, page 41, lines 4-5 and FIG. 11, item 1108. The method further comprises generating a third key. *See e.g.* Appellants' specification, page 41, lines 26-29. The method further comprises applying to the first ciphertext packet a third cryptographic algorithm with the third key to convert the first ciphertext packet to a second ciphertext packet having three layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet. *See e.g.* Appellants' specification, page 41, lines 5-12.

Embodiments according to independent claim 120 describe a receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets. The receiver comprises an input port adapted to receive a first key and a second key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has two layers of encryption thereon that were applied by a first cryptographic algorithm using the first key and a second cryptographic algorithm using the second key. *See e.g.* Appellants' specification, page 40, lines 17-20, page 41, lines 4-5 and FIG. 11, item 1108. The receiver further comprises a key generator adapted to generate a third key. *See e.g.* Appellants' specification, page 38, lines 17-18, page 41, lines 26-29, and FIG. 7, item 708. The receiver further comprises a cryptographic device in communication with the input port and the

key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a third cryptographic algorithm and the third key without first converting the first ciphertext packet received from the headend to a cleartext packet. *See e.g.* Appellants' specification, page 38, lines 3-9, page 41, lines 5-12 and FIGS. 6-7, item 610. The receiver further comprises a storage device in communication with the cryptographic device adapted to store the second ciphertext packet and the first, second and third keys. *See e.g.* Appellants' specification, page 26, line 31 – page 27, line 11 and FIG. 6, item 614.

VI. Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejections are to be reviewed on appeal:

Claims 55-76, 83-91, and 105-124 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Rabowsky* (U.S. Pat. No. 6,141,530, hereinafter "*Rabowsky*") in view of *Bartholet et al.* (U.S. Pub. No. 2002/0114453, hereinafter "*Bartholet*").

VII. Arguments

For the reasons that follow, Appellants request that the rejections of claims 55-76, 83-91, and 105-124 be overturned.

A. Rejection of Claims 55-76, 83-91, and 105-124 under 35 U.S.C. §103(a): *Rabowsky* and *Bartholet*

1. Appellants' Claim 55

Appellants' claim 55 provides as follows (emphasis added):

> A method for securely storing encrypted programming received at a receiver in a subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:
>
> ***receiving a first ciphertext packet having multiple layers of encryption thereon at the receiver***; and
>
> applying a cryptographic algorithm to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting ***the first ciphertext packet received from the headend*** to a cleartext packet.

Appellants respectfully submit that independent claim 55 is allowable for at least the reason that *Rabowsky* in view of *Bartholet* does not disclose, teach, or suggest at least the features recited and emphasized above in claim 55.

The final Office Action alleges on page 4 that "Rabowski discloses: receiving from a headend of the subscriber network a first ciphertext packet at the receiver". However, the final Office Action fails to even allege that the cited references teach "receiving a first ciphertext packet having multiple layers of encryption thereon at the receiver" (emphasis added) as recited

in claim 55. Rather, the final Office Action alleges on page 5 that "Bartholet... discloses... the received encrypted packets are further encrypted ... where multi-layer encryption may be employed". Appellants respectfully submit that encrypting received packets with multi-layer encryption is not the same as "receiving a first ciphertext packet having multiple layers of encryption thereon".

Further, the Advisory Action acknowledges on page 2 that "Rabowsky does not expressly teach a scheme to encrypt data more than one time", however the Advisory Action further alleges on page 2 that "Bartholet et al. suggests a multi-layer encryprtion [*sic*] scheme to be performed on the data being transmitted (see, e.g., [0022])." Appellants respectfully disagree. Specifically, *Bartholet* teaches:

> a first gateway in situ generator may ... directly pass [incoming data] ... still encrypted to a separate storage in situ key generator. A separate storage in situ generator may ... further encrypt the data with an additional layer of encryption...
>
> Encryption for storage may be common with or unique from encryption for transmission to and from storage. Multi-layer encryption may be employed ...

(Paragraphs 0012 and 0022). Even assuming, *arguendo*, that *Bartholet* teaches multi-layer encryption for storage, *Bartholet* does not disclose or suggest that the received data has multiple layers of encryption. Thus, *Rabowsky* in view of *Bartholet* does not teach or suggest "receiving a first ciphertext packet having multiple layers of encryption thereon at the receiver... the first ciphertext packet received from the headend" as recited in claim 55.

For at least the reasons described above, *Rabowsky* in view of *Bartholet* fails to disclose, teach or suggest all of the features recited in claim 55. Therefore, Appellants respectfully request that the rejection of claim 55 be overturned.

Moreover, the final Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer

> encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

However, Appellants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). Appellants respectfully submit that, even though the Office Action proffers an alleged motivation ("to raise the cost of the known-plaintext attack"), other than the Advisory Action's conclusory statement that "these two arts are from an analogous field of technology and are combinable" (Advisory Action on page 2), the final Office Action and the Advisory Action provide no support for the motivation to combine the cited references as alleged.

According to well-established case law, "The mere fact that references can be combined or modified does not render the resultant combination obvious unless the results would have been predictable to one of ordinary skill in the art." *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, ___, 82 USPQ2d 1385, 1396 (2007). "[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR*, 550 U.S. at ___, 82 USPQ2d at 1396 quoting *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). Thus, Appellants respectfully submit that one having ordinary skill in the art would not reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, Appellants respectfully submit that the Office Action fails to provide a proper motivation to combine the *Rabowsky* and *Bartholet* references and, therefore, a *prima facie* case of obviousness is not established.

Furthermore, according to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Appellants respectfully note that *Rabowsky* (*see, e.g.*, col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rabowsky* (*see, e.g.*, col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features:

> The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system, receiver-decoders which receive the radio frequency bit stream and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as authorized by the management system, and a reverse channel which provides data back to the headend system from the theaters.

(Emphasis added). In other words, *Rabowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rabowsky* shows a conditional access module 72 residing in the theater referenced above, and col. 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rabowsky*, the headend appears *arguendo* to provide or distribute entitlement information (*e.g.*, headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (*e.g.*, as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet*:

> Often, the process of key distribution for data transfer or storage, results in either unintentional disclosure of the keys to third parties or interception/extraction of the keys or key material by unauthorized entities... Additionally, complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the cost of maintaining a cryptographic communication or data storage system.
>
> The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an innovative alternative to conventional methods of key management. In particular, the inventions facilitate an infrastructure within which data is secured using in situ generated encryption and decryption keys... substantially eliminating any need for key distribution and capable of keeping the keys unknown to all parties involved... By using the in situ pseudo-random key generators, no encryption/decryption keys need be transferred between users...the users may communicate with each other in encryption mode without ever having to transmit the keys over the communication lines.
>
> No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

(Paragraphs 0008, 0009, and 00115; emphasis added). Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rabowsky*, but also operates in a completely different manner than *Rabowsky*. Paragraph [0032] from *Bartholet* provides as follows:

> In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key by only one of the three decryptors. This known information in the data

> may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

(Emphasis added). In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rabowsky*'s disclosed systems and methods, and hence, the references are not properly combinable.

Further, because the claim requires that keys be passed from the headend to the receiver, it is clear that *Bartholet* teaches away from such an implementation, as set forth in the cited and emphasized sections of *Bartholet*. Even assuming *arguendo* one may unreasonably view the disclosure of *Bartholet* as not teaching away the passing of keys from headend to receiver, the combination of *Bartholet* and *Rabowsky* is improper for other reasons (*see, e.g.*, 2143.01 and reproduced below in part):

> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

Clearly, key generation in *Bartholet* is remote from the external terminal. To use keys passed from a headend obviates the need for the gateway 106, as well as obviates the need to pass the time or event information, and ultimately changes the principle of operation of *Bartholet*. For at least this additional reason, Appellants respectfully submit that the combination is improper.

Accordingly, for at least these reasons, the proposed combination of *Rabowsky* in view of *Bartholet* is improper and a *prima facie* case of obviousness is not established. Therefore, Appellants respectfully request that the rejection of claim 55 be overturned.

2. Appellants' Claims 56-68

Since independent claim 55 is allowable, Appellants respectfully submit that claims 56-68 are allowable for at least the reason that each depends from an allowable claim. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q. 2d 1596, 1598 (Fed. Cir.1988). Therefore, Appellants respectfully request that the rejection of claims 56-68 be overturned.

3. Appellants' Claim 69

Appellants' claim 69 provides as follows (emphasis added):

> A method for providing a subscriber of a subscriber network with a program, the subscriber network including a headend with a plurality of receivers coupled thereto, ***at the headend*** the method comprising the steps of:
> receiving a first ciphertext packet;
> ***applying a cryptographic algorithm with a key to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received at the headend to a cleartext packet***;
> transmitting the second ciphertext packet; and
> ***at the receiver*** the method comprising the steps of:
> ***receiving the second ciphertext packet having multiple layers of encryption thereon***; and
> applying a second cryptographic algorithm to the second ciphertext packet to convert the second ciphertext packet to a third ciphertext packet without first converting the second ciphertext packet to a cleartext packet.

Appellants respectfully submit that independent claim 69 is allowable for at least the reason that *Rabowsky* in view of *Bartholet* does not disclose, teach, or suggest at least the features recited and emphasized above in claim 69.

The final Office Action alleges on page 4 that "Rabowski discloses: receiving from a headend of the subscriber network a first ciphertext packet at the receiver". However, the final Office Action fails to even allege that the cited references teach "receiving the second ciphertext packet having multiple layers of encryption thereon" (emphasis added) as recited in claim 69. Rather, the final Office Action alleges on page 5 that "Bartholet... discloses... the received encrypted packets are further encrypted ... where multi-layer encryption may be employed".

Appellants respectfully submit that encrypting received packets with multi-layer encryption is not the same as "receiving the second ciphertext packet having multiple layers of encryption thereon".

Further, the Advisory Action acknowledges on page 2 that "Rabowsky does not expressly teach a scheme to encrypt data more than one time", however the Advisory Action further alleges on page 2 that "Bartholet et al. suggests a multi-layer encryprtion [*sic*] scheme to be performed on the data being transmitted (see, e.g., [0022])." Appellants respectfully disagree. Specifically, *Bartholet* teaches:

> a first gateway in situ generator may ... directly pass [incoming data] ... still encrypted to a separate storage in situ key generator. A separate storage in situ generator may ... further encrypt the data with an additional layer of encryption...
>
> Encryption for storage may be common with or unique from encryption for transmission to and from storage. Multi-layer encryption may be employed ...

(Paragraphs 0012 and 0022). Even assuming, *arguendo*, that *Bartholet* teaches multi-layer encryption for storage, *Bartholet* does not disclose or suggest that the received data has multiple layers of encryption. Nor does *Bartholet* teach or suggest "applying a cryptographic algorithm with a key to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received at the headend to a cleartext packet". Thus, *Rabowsky* in view of *Bartholet* does not teach or suggest either "at the headend ... applying a cryptographic algorithm with a key to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received at the headend to a cleartext packet" or "at the receiver ... receiving the second ciphertext packet having multiple layers of encryption thereon" as recited in claim 69.

For at least the reasons described above, *Rabowsky* in view of *Bartholet* fails to disclose, teach or suggest all of the features recited in claim 69. Therefore, Appellants respectfully request that the rejection of claim 69 be overturned.

Moreover, for the reasons discussed above, Appellants respectfully submit that the Office Action fails to provide a proper motivation to combine the *Rabowsky* and *Bartholet* references and, therefore, a *prima facie* case of obviousness is not established. Moreover, for the reasons discussed above, Appellants respectfully submit that *Bartholet*'s arrangement for the distribution of keys teaches away from *Rabowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, the proposed combination of *Rabowsky* in view of *Bartholet* is improper and a *prima facie* case of obviousness is not established. Therefore, Appellants respectfully request that the rejection of claim 69 be overturned.

4. Appellants' Claims 70-76

Since independent claim 69 is allowable, Appellants respectfully submit that claims 70-76 are allowable for at least the reason that each depends from an allowable claim. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q. 2d 1596, 1598 (Fed. Cir.1988). Therefore, Appellants respectfully request that the rejection of claims 70-76 be overturned.

5. Appellants' Claim 83

Appellants' claim 83 provides as follows (emphasis added):

> A receiver in a subscriber network that receives encrypted programming from a headend of the subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, ***the receiver comprising***:
>
> ***a port adapted to receive a first ciphertext packet of the encrypted programming, the first ciphertext packet corresponding to a cleartext packet having multiple layers of encryption thereon***;
>
> a key generator adapted to generate an encryption key; and
>
> a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to apply a cryptographic algorithm using the encryption key to the first ciphertext packet to convert the ciphertext packet to a second ciphertext packet without first

> converting ***the first ciphertext packet received from the headend*** to a cleartext packet.

Appellants respectfully submit that independent claim 83 is allowable for at least the reason that *Rabowsky* in view of *Bartholet* does not disclose, teach, or suggest at least the features recited and emphasized above in claim 83.

The final Office Action alleges on page 4 that "Rabowski discloses: receiving from a headend of the subscriber network a first ciphertext packet at the receiver". However, the final Office Action fails to even allege that the cited references teach "receiv[ing] a first ciphertext packet ... corresponding to a cleartext packet having multiple layers of encryption thereon" (emphasis added) as recited in claim 83. Rather, the final Office Action alleges on page 5 that "Bartholet... discloses... the received encrypted packets are further encrypted ... where multi-layer encryption may be employed". Appellants respectfully submit that encrypting received packets with multi-layer encryption is not the same as "receiv[ing] a first ciphertext packet ... corresponding to a cleartext packet having multiple layers of encryption thereon".

Further, the Advisory Action acknowledges on page 2 that "Rabowsky does not expressly teach a scheme to encrypt data more than one time", however the Advisory Action further alleges on page 2 that "Bartholet et al. suggests a multi-layer encryprtion [*sic*] scheme to be performed on the data being transmitted (see, e.g., [0022])." Appellants respectfully disagree. Specifically, *Bartholet* teaches:

> a first gateway in situ generator may ... directly pass [incoming data] ... still encrypted to a separate storage in situ key generator. A separate storage in situ generator may ... further encrypt the data with an additional layer of encryption...
>
> Encryption for storage may be common with or unique from encryption for transmission to and from storage. Multi-layer encryption may be employed ...

(Paragraphs 0012 and 0022). Even assuming, *arguendo*, that *Bartholet* teaches multi-layer encryption for storage, *Bartholet* does not disclose or suggest that the received data has multiple layers of encryption. Thus, *Rabowsky* in view of *Bartholet* does not teach or suggest

"the receiver comprising: a port adapted to receive a first ciphertext packet of the encrypted programming, the first ciphertext packet corresponding to a cleartext packet having multiple layers of encryption thereon... the first ciphertext packet received from the headend" as recited in claim 83.

For at least the reasons described above, *Rabowsky* in view of *Bartholet* fails to disclose, teach or suggest all of the features recited in claim 83. Therefore, Appellants respectfully request that the rejection of claim 83 be overturned.

Moreover, for the reasons discussed above, Appellants respectfully submit that the Office Action fails to provide a proper motivation to combine the *Rabowsky* and *Bartholet* references and, therefore, a *prima facie* case of obviousness is not established. Moreover, for the reasons discussed above, Appellants respectfully submit that *Bartholet*'s arrangement for the distribution of keys teaches away from *Rabowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, the proposed combination of *Rabowsky* in view of *Bartholet* is improper and a *prima facie* case of obviousness is not established. Therefore, Appellants respectfully request that the rejection of claim 83 be overturned.

6. Appellants' Claims 84-91

Since independent claim 83 is allowable, Appellants respectfully submit that claims 84-91 are allowable for at least the reason that each depends from an allowable claim. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q. 2d 1596, 1598 (Fed. Cir.1988). Therefore, Appellants respectfully request that the rejection of claims 84-91 be overturned.

7. Appellants' Claim 105

Appellants' claim 105 provides as follows (emphasis added):

> A method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:

> ***receiving from a headend of the subscriber network a first ciphertext packet at the receiver and a first key, a second key and a third key, wherein the first ciphertext packet has three layers of encryption thereon*** that were applied by a first cryptographic algorithm using the first key, the second key and the third key;
>
> generating a fourth key;
>
> ***applying to the first ciphertext packet a second cryptographic algorithm with the first key to convert the first ciphertext packet to a second ciphertext packet having two layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet***; and
>
> applying to the second ciphertext packet a third cryptographic algorithm with the fourth key to convert the second ciphertext packet to a third ciphertext packet having a third layer of encryption thereon without first converting the second ciphertext packet to a cleartext packet.

Appellants respectfully submit that independent claim 105 is allowable for at least the reason that *Rabowsky* in view of *Bartholet* does not disclose, teach, or suggest at least the features recited and emphasized above in claim 105.

The final Office Action alleges on page 4 that "Rabowski discloses: receiving from a headend of the subscriber network a first ciphertext packet at the receiver". However, the final Office Action fails to even allege that the cited references teach "receiving ... a first ciphertext packet ... wherein the first ciphertext packet has three layers of encryption thereon" (emphasis added) as recited in claim 105. Rather, the final Office Action alleges on page 5 that "Bartholet... discloses... the received encrypted packets are further encrypted ... where multi-layer encryption may be employed". Appellants respectfully submit that encrypting received packets with multi-layer encryption is not the same as "receiving ... a first ciphertext packet ... wherein the first ciphertext packet has three layers of encryption thereon".

Further, the Advisory Action acknowledges on page 2 that "Rabowsky does not expressly teach a scheme to encrypt data more than one time", however the Advisory Action further alleges on page 2 that "Bartholet et al. suggests a multi-layer encryprtion [*sic*] scheme to be performed on the data being transmitted (see, e.g., [0022])." Appellants respectfully disagree. Specifically, *Bartholet* teaches:

> a first gateway in situ generator may ... directly pass [incoming data] ... still encrypted to a separate storage in situ key generator. A separate storage in situ generator may ... further encrypt the data with an additional layer of encryption...
>
> Encryption for storage may be common with or unique from encryption for transmission to and from storage. Multi-layer encryption may be employed ...

(Paragraphs 0012 and 0022). Even assuming, *arguendo*, that *Bartholet* teaches multi-layer encryption for storage, *Bartholet* does not disclose or suggest that the received data has multiple layers of encryption. Thus, *Rabowsky* in view of *Bartholet* does not teach or suggest "receiving from a headend of the subscriber network a first ciphertext packet at the receiver and a first key, a second key and a third key, wherein the first ciphertext packet has three layers of encryption thereon" as recited in claim 105.

Additionally, the final Office Action alleges on page 4 that "Rabowski discloses... an input port adapted to receive a first key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has a single layer of encryption thereon that was applied by a first cryptographic algorithm using the first key". However, the final Office Action fails to even allege that the cited references teach "applying to the first ciphertext packet a second cryptographic algorithm with the first key to convert the first ciphertext packet to a second ciphertext packet having two layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet" (emphasis added) as recited in claim 105. As noted above, the Advisory Action acknowledges on page 2 that "Rabowsky does not expressly teach a scheme to encrypt data more than one time".

Furthermore, *Bartholet* does not teach or suggest "receiving from a headend ... a first key ... [and] applying to the first ciphertext packet a second cryptographic algorithm with the first key to convert the first ciphertext packet to a second ciphertext packet having two layers of encryption thereon". Rather, *Bartholet* teaches that "No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since

all the keys are internally generated by the in situ key generators" (paragraph 0015; emphasis added). Thus, *Rabowsky* in view of *Bartholet* does not disclose or suggest "applying to the first ciphertext packet a second cryptographic algorithm with the first key to convert the first ciphertext packet to a second ciphertext packet having two layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet" as recited in claim 105.

For at least the reasons described above, *Rabowsky* in view of *Bartholet* fails to disclose, teach or suggest all of the features recited in claim 105. Therefore, Appellants respectfully request that the rejection of claim 105 be overturned.

Moreover, for the reasons discussed above, Appellants respectfully submit that the Office Action fails to provide a proper motivation to combine the *Rabowsky* and *Bartholet* references and, therefore, a *prima facie* case of obviousness is not established. Moreover, for the reasons discussed above, Appellants respectfully submit that *Bartholet*'s arrangement for the distribution of keys teaches away from *Rabowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, the proposed combination of *Rabowsky* in view of *Bartholet* is improper and a *prima facie* case of obviousness is not established. Therefore, Appellants respectfully request that the rejection of claim 105 be overturned.

8. Appellants' Claims 106-109

Since independent claim 105 is allowable, Appellants respectfully submit that claims 106-109 are allowable for at least the reason that each depends from an allowable claim. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q. 2d 1596, 1598 (Fed. Cir.1988). Therefore, Appellants respectfully request that the rejection of claims 106-109 be overturned.

9. Appellants' Claim 110

Appellants' claim 110 provides as follows (emphasis added):

> A receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:
>
> ***an input port adapted to receive a first key, a second key, a third key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has three layers of encryption thereon*** that were applied by a first cryptographic algorithm using the first key, a second key and a third key;
>
> a key generator adapted to generate a fourth key;
>
> ***a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a second cryptographic algorithm and the first key without first converting the first ciphertext packet received from the headend to a cleartext packet*** and thereafter to convert the second ciphertext packet to a third ciphertext packet using a third cryptographic algorithm and the fourth key without first converting the second ciphertext packet to a cleartext packet; and
>
> a storage device in communication with the cryptographic device adapted to store the third ciphertext packet and the second, third and fourth keys.

Appellants respectfully submit that independent claim 110 is allowable for at least the reason that *Rabowsky* in view of *Bartholet* does not disclose, teach, or suggest at least the features recited and emphasized above in claim 110.

The final Office Action alleges on page 4 that "Rabowski discloses: receiving from a headend of the subscriber network a first ciphertext packet at the receiver". However, the final Office Action fails to even allege that the cited references teach "receiv[ing] ... a first ciphertext ... wherein the first ciphertext packet has three layers of encryption thereon" (emphasis added) as recited in claim 110. Rather, the final Office Action alleges on page 5 that "Bartholet... discloses... the received encrypted packets are further encrypted ... where multi-layer encryption may be employed". Appellants respectfully submit that encrypting received packets with multi-layer encryption is not the same as "receiv[ing] ... a first ciphertext ... wherein the first ciphertext packet has three layers of encryption thereon".

Further, the Advisory Action acknowledges on page 2 that "Rabowsky does not expressly teach a scheme to encrypt data more than one time", however the Advisory Action further alleges on page 2 that "Bartholet et al. suggests a multi-layer encryprtion [*sic*] scheme to be performed on the data being transmitted (see, e.g., [0022])." Appellants respectfully disagree. Specifically, *Bartholet* teaches:

> a first gateway in situ generator may ... directly pass [incoming data] ... still encrypted to a separate storage in situ key generator. A separate storage in situ generator may ... further encrypt the data with an additional layer of encryption...
>
> Encryption for storage may be common with or unique from encryption for transmission to and from storage. Multi-layer encryption may be employed ...

(Paragraphs 0012 and 0022). Even assuming, *arguendo*, that *Bartholet* teaches multi-layer encryption for storage, *Bartholet* does not disclose or suggest that the received data has multiple layers of encryption. Thus, *Rabowsky* in view of *Bartholet* does not teach or suggest "an input port adapted to receive a first key, a second key, a third key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has three layers of encryption thereon" as recited in claim 110.

Additionally, the final Office Action alleges on page 4 that "Rabowski discloses... an input port adapted to receive a first key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has a single layer of encryption thereon that was applied by a first cryptographic algorithm using the first key ... [and] a cryptographic device in communication with the input port and the key generator". However, the final Office Action fails to even allege that the cited references teach "the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a second cryptographic algorithm and the first key without first converting the first ciphertext packet received from the headend to a cleartext packet" (emphasis added) as recited in claim 110. As noted above, the Advisory Action

acknowledges on page 2 that "Rabowsky does not expressly teach a scheme to encrypt data more than one time".

Furthermore, *Bartholet* does not teach or suggest "an input port adapted to receive a first key... [and] the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a second cryptographic algorithm and the first key without first converting the first ciphertext packet received from the headend to a cleartext packet". Rather, *Bartholet* teaches that "No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators" (paragraph 0015; emphasis added). Thus, *Rabowsky* in view of *Bartholet* does not disclose or suggest "a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a second cryptographic algorithm and the first key without first converting the first ciphertext packet received from the headend to a cleartext packet" as recited in claim 110.

For at least the reasons described above, *Rabowsky* in view of *Bartholet* fails to disclose, teach or suggest all of the features recited in claim 110. Therefore, Appellants respectfully request that the rejection of claim 110 be overturned.

Moreover, for the reasons discussed above, Appellants respectfully submit that the Office Action fails to provide a proper motivation to combine the *Rabowsky* and *Bartholet* references and, therefore, a *prima facie* case of obviousness is not established. Moreover, for the reasons discussed above, Appellants respectfully submit that *Bartholet*'s arrangement for the distribution of keys teaches away from *Rabowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, the proposed combination of *Rabowsky* in view of *Bartholet* is improper and a *prima facie* case of obviousness is not established. Therefore, Appellants respectfully request that the rejection of claim 110 be overturned.

10. Appellants' Claims 111-114

Since independent claim 110 is allowable, Appellants respectfully submit that claims 111-114 are allowable for at least the reason that each depends from an allowable claim. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q. 2d 1596, 1598 (Fed. Cir.1988). Therefore, Appellants respectfully request that the rejection of claims 111-114 be overturned.

11. Appellants' Claim 115

Appellants' claim 115 provides as follows (emphasis added):

> A method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:
> ***receiving from a headend of the subscriber network a first ciphertext packet at the receiver*** and a first key and a second key***, wherein the first ciphertext packet has two layers of encryption thereon*** that were applied by a first cryptographic algorithm using the first key and a second cryptographic algorithm using the second key;
> generating a third key; and
> applying to the first ciphertext packet a third cryptographic algorithm with the third key to convert the first ciphertext packet to a second ciphertext packet having three layers of encryption thereon without first converting ***the first ciphertext packet received from the headend*** to a cleartext packet.

Appellants respectfully submit that independent claim 115 is allowable for at least the reason that *Rabowsky* in view of *Bartholet* does not disclose, teach, or suggest at least the features recited and emphasized above in claim 115.

The final Office Action alleges on page 4 that "Rabowski discloses: receiving from a headend of the subscriber network a first ciphertext packet at the receiver". However, the final Office Action fails to even allege that the cited references teach "receiving ... a first ciphertext packet at the receiver ... wherein the first ciphertext packet has two layers of encryption thereon" (emphasis added) as recited in claim 115. Rather, the final Office Action alleges on page 5 that "Bartholet... discloses... the received encrypted packets are further encrypted ... where multi-layer encryption may be employed". Appellants respectfully submit that encrypting received

packets with multi-layer encryption is not the same as "receiving ... a first ciphertext packet at the receiver ... wherein the first ciphertext packet has two layers of encryption thereon".

Further, the Advisory Action acknowledges on page 2 that "Rabowsky does not expressly teach a scheme to encrypt data more than one time", however the Advisory Action further alleges on page 2 that "Bartholet et al. suggests a multi-layer encryprtion [*sic*] scheme to be performed on the data being transmitted (see, e.g., [0022])." Appellants respectfully disagree. Specifically, *Bartholet* teaches:

> a first gateway in situ generator may ... directly pass [incoming data] ... still encrypted to a separate storage in situ key generator. A separate storage in situ generator may ... further encrypt the data with an additional layer of encryption...
>
> Encryption for storage may be common with or unique from encryption for transmission to and from storage. Multi-layer encryption may be employed ...

(Paragraphs 0012 and 0022). Even assuming, *arguendo*, that *Bartholet* teaches multi-layer encryption for storage, *Bartholet* does not disclose or suggest that the received data has multiple layers of encryption. Thus, *Rabowsky* in view of *Bartholet* does not teach or suggest "receiving from a headend of the subscriber network a first ciphertext packet at the receiver ... wherein the first ciphertext packet has two layers of encryption thereon ... the first ciphertext packet received from the headend" as recited in claim 115.

For at least the reasons described above, *Rabowsky* in view of *Bartholet* fails to disclose, teach or suggest all of the features recited in claim 115. Therefore, Appellants respectfully request that the rejection of claim 115 be overturned.

Moreover, for the reasons discussed above, Appellants respectfully submit that the Office Action fails to provide a proper motivation to combine the *Rabowsky* and *Bartholet* references and, therefore, a *prima facie* case of obviousness is not established. Moreover, for the reasons discussed above, Appellants respectfully submit that *Bartholet*'s arrangement for the distribution of keys teaches away from *Rabowsky*'s disclosed systems and methods, and hence,

the references are not properly combinable. Accordingly, the proposed combination of *Rabowsky* in view of *Bartholet* is improper and a *prima facie* case of obviousness is not established. Therefore, Appellants respectfully request that the rejection of claim 115 be overturned.

12. Appellants' Claims 116-119

Since independent claim 115 is allowable, Appellants respectfully submit that claims 116-119 are allowable for at least the reason that each depends from an allowable claim. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q. 2d 1596, 1598 (Fed. Cir.1988). Therefore, Appellants respectfully request that the rejection of claims 116-119 be overturned.

13. Appellants' Claim 120

Appellants' claim 120 provides as follows (emphasis added):

> A receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets, ***the receiver comprising***:
> ***an input port adapted to receive a first key and a second key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has two layers of encryption thereon*** that were applied by a first cryptographic algorithm using the first key and a second cryptographic algorithm using the second key;
> a key generator adapted to generate a third key;
> a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a third cryptographic algorithm and the third key without first converting ***the first ciphertext packet received from the headend*** to a cleartext packet; and
> a storage device in communication with the cryptographic device adapted to store the second ciphertext packet and the first, second and third keys.

Appellants respectfully submit that independent claim 120 is allowable for at least the reason that *Rabowsky* in view of *Bartholet* does not disclose, teach, or suggest at least the features recited and emphasized above in claim 120.

The final Office Action alleges on page 4 that "Rabowski discloses: receiving from a headend of the subscriber network a first ciphertext packet at the receiver". However, the final

Office Action fails to even allege that the cited references teach "receiv[ing] ... a first ciphertext ... wherein the first ciphertext packet has two layers of encryption thereon" (emphasis added) as recited in claim 120. Rather, the final Office Action alleges on page 5 that "Bartholet... discloses... the received encrypted packets are further encrypted ... where multi-layer encryption may be employed". Appellants respectfully submit that encrypting received packets with multi-layer encryption is not the same as "receiv[ing] ... a first ciphertext ... wherein the first ciphertext packet has two layers of encryption thereon".

Further, the Advisory Action acknowledges on page 2 that "Rabowsky does not expressly teach a scheme to encrypt data more than one time", however the Advisory Action further alleges on page 2 that "Bartholet et al. suggests a multi-layer encryprtion [*sic*] scheme to be performed on the data being transmitted (see, e.g., [0022])." Appellants respectfully disagree. Specifically, *Bartholet* teaches:

> a first gateway in situ generator may ... directly pass [incoming data] ... still encrypted to a separate storage in situ key generator. A separate storage in situ generator may ... further encrypt the data with an additional layer of encryption...
>
> Encryption for storage may be common with or unique from encryption for transmission to and from storage. Multi-layer encryption may be employed ...

(Paragraphs 0012 and 0022). Even assuming, *arguendo*, that *Bartholet* teaches multi-layer encryption for storage, *Bartholet* does not disclose or suggest that the received data has multiple layers of encryption. Thus, *Rabowsky* in view of *Bartholet* does not teach or suggest "the receiver comprising: an input port adapted to receive a first key and a second key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has two layers of encryption thereon ... the first ciphertext packet received from the headend" as recited in claim 120.

For at least the reasons described above, *Rabowsky* in view of *Bartholet* fails to disclose, teach or suggest all of the features recited in claim 120. Therefore, Appellants respectfully request that the rejection of claim 120 be overturned.

Moreover, for the reasons discussed above, Appellants respectfully submit that the Office Action fails to provide a proper motivation to combine the *Rabowsky* and *Bartholet* references and, therefore, a *prima facie* case of obviousness is not established. Moreover, for the reasons discussed above, Appellants respectfully submit that *Bartholet*'s arrangement for the distribution of keys teaches away from *Rabowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, the proposed combination of *Rabowsky* in view of *Bartholet* is improper and a *prima facie* case of obviousness is not established. Therefore, Appellants respectfully request that the rejection of claim 120 be overturned.

14. Appellants' Claims 121-124

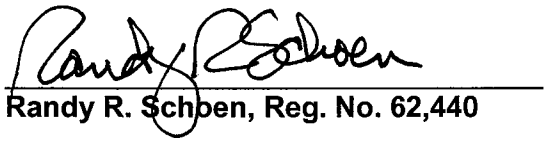
Since independent claim 120 is allowable, Appellants respectfully submit that claims 121-124 are allowable for at least the reason that each depends from an allowable claim. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q. 2d 1596, 1598 (Fed. Cir.1988). Therefore, Appellants respectfully request that the rejection of claims 121-124 be overturned.

Conclusion

In summary, it is Appellants' position that Appellants' claims are patentable over the applied cited art references and that the rejection of these claims should be overturned. Appellants therefore respectfully request that the Board of Appeals overturn the Examiner's rejection and allow Appellants' pending claims.

In addition to the claims shown in the claims Appendix VIII, Appendix IX attached hereto indicates that there is no evidence being attached and relied upon by this brief. Appendix X attached hereto indicates that there are no related proceedings.

Respectfully submitted,

By: 
Randy R. Schben, Reg. No. 62,440

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.
600 Galleria Parkway, SE
Suite 1500
Atlanta, Georgia 30339-5948
Tel: (770) 933-9500
Fax: (770) 951-0933

VIII. Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)

55. A method for securely storing encrypted programming received at a receiver in a subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:

receiving a first ciphertext packet having multiple layers of encryption thereon at the receiver; and

applying a cryptographic algorithm to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet.

56. The method of claim 55, wherein the second ciphertext packet corresponds to a cleartext packet that was encrypted using a second cryptographic algorithm.

57. The method of claim 56, wherein the second cryptographic algorithm is a 3DES cryptographic algorithm.

58. The method of claim 55, wherein the multiple layers of an encryption include a first layer and a second layer.

59. The method of claim 58, wherein the first layer of encryption corresponds to applying a second cryptographic algorithm to convert a cleartext packet to a third ciphertext packet.

60. The method of claim 59, wherein the second cryptographic algorithm is a DES algorithm.

61. The method of claim 59, wherein the second layer of encryption corresponds to applying a third cryptographic algorithm to convert the third ciphertext packet to the first ciphertext packet.

62. The method of claim 61, wherein the third cryptographic algorithm is a DES algorithm.

63. The method of claim 55, further including the steps of:

applying a second cryptographic algorithm to the second ciphertext packet to convert the second ciphertext packet to a cleartext packet.

64. The method of claim 63, wherein the second cryptographic algorithm is a 3DES algorithm.

65. The method of claim 63, further including the step of:

converting the cleartext packet from a first format to a second format.

66. The method of claim 65, wherein the first format is an MPEG format.

67. The method of claim 55, further including the step of:

receiving multiple keys, each key associated with at least one layer of encryption of the first ciphertext packet.

68. The method of claim 55, further including the step of:

generating a key for use with the cryptographic algorithm.

69. A method for providing a subscriber of a subscriber network with a program, the subscriber network including a headend with a plurality of receivers coupled thereto, at the headend the method comprising the steps of:

receiving a first ciphertext packet;

applying a cryptographic algorithm with a key to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received at the headend to a cleartext packet;

transmitting the second ciphertext packet; and

at the receiver the method comprising the steps of:

receiving the second ciphertext packet having multiple layers of encryption thereon; and

applying a second cryptographic algorithm to the second ciphertext packet to convert the second ciphertext packet to a third ciphertext packet without first converting the second ciphertext packet to a cleartext packet.

70. The method of claim 69, wherein the first ciphertext packet corresponds to a cleartext packet that was encrypted by a third cryptographic algorithm using a second key.

71. The method of claim 70, wherein the first, the second and the third cryptographic algorithms are the same.

72. The method of claim 71, wherein the first cryptographic algorithm is a DES algorithm.

73. The method of claim 69, wherein the third ciphertext packet corresponds to a cleartext packet that was encrypted using a forth cryptographic algorithm.

74. The method of claim 73, wherein the fourth cryptographic algorithm is a 3DES cryptographic algorithm.

75. The method of claim 69, at the receiver, further including the step of:

applying a third cryptographic algorithm to the third ciphertext packet to convert the third ciphertext packet to a cleartext packet.

76. The method of claim 75, wherein the third cryptographic algorithm is a 3DES algorithm.

83. A receiver in a subscriber network that receives encrypted programming from a headend of the subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:

a port adapted to receive a first ciphertext packet of the encrypted programming, the first ciphertext packet corresponding to a cleartext packet having multiple layers of encryption thereon;

a key generator adapted to generate an encryption key; and

a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to apply a cryptographic algorithm using the encryption key to the first ciphertext packet to convert the ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet.

84. The receiver of claim 83, further including:

a storage device in communication with the cryptographic device, the storage device adapted to store the second ciphertext packet and the encryption key.

85. The receiver of claim 83, further including:

an output port in communication with the cryptographic device, the output port adapted to interface with external storage devices.

86. The receiver of claim 83, wherein the cryptographic algorithm is a DES algorithm.

87. The receiver of claim 83, wherein the second ciphertext packet corresponds to a cleartext packet encrypted by a 3DES algorithm.

88. The receiver of claim 83, wherein the input port is adapted to receive at least one decryption key, and the cryptographic device is adapted to use the at least one decryption key with the encryption key and a second cryptographic algorithm to convert the second ciphertext packet to the corresponding cleartext packet.

89. The receiver of claim 88, wherein the second cryptographic algorithm is a 3DES algorithm.

90. The receiver of claim 88, further including:

a converter adapted to convert the cleartext packet from a first format to a second format.

91. The receiver of claim 90, wherein the first format is an MPEG format.

105. A method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:

receiving from a headend of the subscriber network a first ciphertext packet at the receiver and a first key, a second key and a third key, wherein the first ciphertext packet has three layers of encryption thereon that were applied by a first cryptographic algorithm using the first key, the second key and the third key;

generating a fourth key;

applying to the first ciphertext packet a second cryptographic algorithm with the first key to convert the first ciphertext packet to a second ciphertext packet having two layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet; and

applying to the second ciphertext packet a third cryptographic algorithm with the fourth key to convert the second ciphertext packet to a third ciphertext packet having a third layer of encryption thereon without first converting the second ciphertext packet to a cleartext packet.

106. The method of claim 105, wherein the receiver is remote from the headend and located at a subscriber location; and further including the step of:

storing the third ciphertext packet and the second, third and fourth keys at the subscriber location.

107. The method of claim 106, further including the steps of:

retrieving the third ciphertext packet and the second, third and fourth keys from storage; and

decrypting the third ciphertext packet by applying a fourth cryptographic algorithm to third ciphertext packet with the second, third and fourth keys, thereby converting the third ciphertext packet to a cleartext packet.

108. The method of claim 107, further including the step of:

converting the cleartext packet from a first format to a second format.

109. The method of claim 108, wherein the first format is an MPEG format.

110. A receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:

an input port adapted to receive a first key, a second key, a third key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has three layers of encryption thereon that were applied by a first cryptographic algorithm using the first key, a second key and a third key;

a key generator adapted to generate a fourth key;

a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a second cryptographic algorithm and the first key without first converting the first ciphertext packet received from the headend to a cleartext packet and thereafter to convert the second ciphertext packet to a third ciphertext packet using a third cryptographic algorithm and the fourth key without first converting the second ciphertext packet to a cleartext packet; and

a storage device in communication with the cryptographic device adapted to store the third ciphertext packet and the second, third and fourth keys.

111. The receiver of claim 110, wherein the cryptographic device is further adapted to decrypt the third ciphertext packet by applying a fourth cryptographic algorithm to the third ciphertext packet with the second, third and fourth keys thereby converting the third ciphertext packet to a cleartext packet.

112. The receiver of claim 111, wherein the first, second and third cryptographic algorithms are a DES algorithm and the fourth cryptographic algorithm is a 3DES algorithm.

113. The receiver of claim 111, further including:

a converter in communication with the cryptographic device adapted to convert the cleartext packet from a first format to a second format.

114. The receiver of claim 113, wherein the first format is an MPEG format.

115. A method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:

receiving from a headend of the subscriber network a first ciphertext packet at the receiver and a first key and a second key, wherein the first ciphertext packet has two layers of encryption thereon that were applied by a first cryptographic algorithm using the first key and a second cryptographic algorithm using the second key;

generating a third key; and

applying to the first ciphertext packet a third cryptographic algorithm with the third key to convert the first ciphertext packet to a second ciphertext packet having three layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet.

116. The method of claim 115, wherein the receiver is remote from the headend and located at a subscriber location; and further including the step of:

storing the third ciphertext packet and the first, second and third keys at the subscriber location.

117. The method of claim 116, further including the steps of:

retrieving the third ciphertext packet and the first, second and third keys from storage; and

decrypting the third ciphertext packet by applying a fourth cryptographic algorithm to third ciphertext packet with the first, second and third keys, thereby converting the third ciphertext packet to a cleartext packet.

118. The method of claim 117, further including the step of:

converting the cleartext packet from a first format to a second format.

119. The method of claim 118, wherein the first format is an MPEG format.

120. A receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:

an input port adapted to receive a first key and a second key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has two layers of encryption thereon that were applied by a first cryptographic algorithm using the first key and a second cryptographic algorithm using the second key;

a key generator adapted to generate a third key;

a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a third cryptographic algorithm and the third key without first converting the first ciphertext packet received from the headend to a cleartext packet; and

a storage device in communication with the cryptographic device adapted to store the second ciphertext packet and the first, second and third keys.

121. The receiver of claim 120, wherein the cryptographic device is further adapted to decrypt the third ciphertext packet by applying a fourth cryptographic algorithm to the third ciphertext packet with the first, second and third keys thereby converting the third ciphertext packet to a cleartext packet.

122. The receiver of claim 121, wherein the first, second and third cryptographic algorithms are a DES algorithm and the fourth cryptographic algorithm is a 3DES algorithm.

123. The receiver of claim 121, further including:

a converter in communication with the cryptographic device adapted to convert the cleartext packet from a first format to a second format.

124. The receiver of claim 123, wherein the first format is an MPEG format.

IX. Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)

None.

X. Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)

None.